SYSTEM AND METHOD FOR FACILITATING TRUSTED TRANSACTIONS BETWEEN BUSINESSES

FIELD OF THE INVENTION

This invention relates to a system and method for facilitating transactions between businesses. In particular, it is concerned with the provision of on-line guarantees by companies engaged in business-to-business (B2B) e-commerce.

BACKGROUND TO THE INVENTION

When two companies transact over a network such as the Internet, some messages that are exchanged require guarantees. A guarantee is an obligation on behalf of one party to fulfil a commitment or an instruction and messages which represent such a commitment or instruction must be guaranteed. As a simple example, a receiver needs a guarantee about a sender's identity and the time and date a message was sent.

In business-to-business (B2B) transactions, companies could rely on their banks to provide such guarantees. Banks already provide loans and financial guarantees to customers. Figure 1 illustrates a scenario where a receiver 10 obtains a guarantee by sending a 'certificate valid' message 12 to the bank 14 who issued the sender's certificate, the bank then sends the guarantee message 16 back to the receiver. This is unattractive as it requires extra work by the receiver who also may not have a relationship with the bank.

SUMMARY OF THE INVENTION

The present invention aims to overcome the abovementioned disadvantages with the prior art method and apparatus.

In accordance with the invention, this aim is met by a system in which a guarantee is added to the message sent to the receiver. This arrangement greatly reduces the amount of messaging required.

In one embodiment of the invention, an intermediate party is arranged between the sending party and the receiving party. The intermediate party receives messages, which may be signed, from the sending party, and obtains a guarantee from a sending party guarantor. The intermediate party then sends the message, as a guaranteed message, to the receiving party.

In one embodiment, the intermediate party also obtains a guarantee from the receiving party guarantor. When a message is received at the receiving party, a receipt is sent to the intermediate party which sends it as a guaranteed receipt to the sending party.

Preferably, on receipt of a message, the intermediate party logs it, adds a timestamp and reference and verifies any signature. It then determines the sender's identity and its guarantor's identity.

Preferably, guaranteed messages are logged before they are sent to the receiving party. The receipts are also logged before being sent by the intermediate party as guaranteed receipts.

Embodiments of the invention have the advantage that message flow is greatly simplified. They have the further advantage that customers can obtain on-line guarantees for e-commerce transactions from banks.

A preferred embodiment has the further advantage that the intermediate party, through its logging, timestamping and referencing of messages, can provide an on-line notarisation enabling resolution of disputes between parties.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, and with reference to the accompanying drawings in which:

Figure 1 is an overview of a known model for providing guarantees;

Figure 2 is an overview of the model for providing guarantees adopted by the present invention;

Figure 3 illustrates the contractual relationship between parties to a transaction;

Figure 4 illustrates the levels of contractual relationships in the system;

Figure 5 illustrates the message flow in a system embodying the present invention;

Figure 6 is a schematic view of the topology of a system embodying the invention.

DESCRIPTION OF PREFERRED EMBODIMENT

Referring to the figures, the purpose of the system is to facilitate trusted business-to-business (B2B) e-commerce by enabling businesses to obtain on-line guarantees from their bank. Banks can use the system to be described to provide on-line guarantees and e-trust services to corporate customers.

The system to be described operates over a communications network, preferably a combination of the Internet and a private network. In essence it is a messaging service which adds guarantees to e-commerce messages, enabling trusted e-commerce.

The system to be described operates on the principle that guarantees are attached before they are received by a receiver. The receiver's guarantor may also be involved. This is illustrated in Figure 2 in which the bank is shown at 14 and the receiver at 10.

Figure 3 shows the contractual relationship between the various parties to a transaction. The sender 20 and receiver 30 each have a contractual relationship with their own guarantors, 22 and 32 Guarantees can be exchanged by the guarantors through a third party 34 establishing an indirect relationship between the sender and the receiver. Such an arrangement may be used to provide more than the provision of identity guarantees and may extend to the provision of on-line notarisation, a legal framework that makes messages binding, and guarantees such as the ability to pay. The system operates by providing a guarantee service to which banks or other institutions sign up as guarantors and businesses sign up as customers.

Messages exchanged between senders and receivers may be made legally binding by establishing contractual relationships between senders and receivers and their banks and by establishing contractual relationships between senders, receivers, their banks and the service providers 34. Message exchange also takes place under the terms of Contract Law.

The contractual relationship between subscribers and guarantors will set out details of service levels, prices, procedures and other factors determining the provision of guarantee services as the guarantor to the subscriber. It may refer to a Certification Practices Statement.

The contractual relationship between the Guarantors and the service providers defines service levels between the service provider and the guarantors as well as defining the service levels the guarantor can promise to provide the subscribers.

This two tier contractual relationship is illustrated in figure 4 with the subscriber shown at 50, the service provider at 60 and the guarantors at 70.

Each of the levels of contract may refer to a rulebook established by the service provider to which the parties are then bound. Thus, the guarantors have an explicit relationship with the service provider 34 and an implied

relationship with other guarantors who have a contractual relationship with the service provider.

Referring to figure 5, the message flow in a transaction will now be described.

The purpose of the following sequence is for the sender to send a signed message to a receiver which is received by the receiver as a guaranteed message.

The first stage is for the sender to send a signed message to the service provider. In figure 5 this is shown by pathway 1. The signed message requires a bank's guarantee and is created by any suitable application at the sender, for example a browser or an ERP system which signs the message and sends it to the service provider.

At the second stage, the service provider receives the signed message from the sender, logs it and adds to it a timestamp and individual reference number. It then verifies the signature using its public key. The use and verification of signed electronic messages is well understood and will not be described further.

The service provider then interprets the received signed message to determine the sender's identity, its public key and the identity of the sender's guarantor. It then establishes a connection to the receiver to obtain its public key and its guarantor's identity. The service provider will then send a guarantee request to the sender's guarantor relative to the sender and to the receiver's guarantor relative to the receiver.

These two guarantee request messages are shown at 2 in figure 5. Thus, in this stage, the service provider 34 has requested guaranteed identity from the guarantors 22,32.

At the next stage, shown as 3 in figure 5, the guarantors confirm, respectively, the identity of the sender and receiver to the service provider. The guarantors each

receive and process the guarantee request made by the service provider and send a guarantee response back to the service provider.

The service provider then forwards the guaranteed message to the receiver as shown at 4 in figure 5. This can take place once the two guarantors have confirmed the guarantee. The service provider constructs a guaranteed message using the original signed message and the timestamp and reference number that were applied when the message was received at the service provider. The guaranteed message is first logged and then sent to the receiver.

The receiver, at 5, receives the guaranteed message from the service provider, authenticates the service provider's signature which is attached to the message and can then rely on that message.

The receiver then acknowledges receipt of the message by returning a signed receipt to the service provider, illustrated at 6 in figure 5. The service provider then constructs a guaranteed receipt by adding the guaranteed identity obtained from the receiver's guarantor to the signed receipt, logs the guaranteed receipt and forwards it to the initial sender. This step is shown at 7 in figure 5.

From the description given above, it will be appreciated that messages passing through the service provider 34 are timestamped and logged. Timestamping guarantees that a message was sent at a universal, commonly accepted time. Logging allows messages to be retrieved at a later date so that disputes can be resolved. Thus, the system and method described can be used to provide an on-line notarisation service.

As mentioned above, the contractual agreement between the various parties may refer to a rulebook. The following description sets out a summary of the major obligations on the subscribers, guarantors and service provide that may be required.

<u>Subscribers</u>

Subscribers are required to manage their keys and security in a responsible manner, for example by maintaining exclusive access to the private key. Senders must send signed messages to the service providers requesting guarantees when asked by the receiver and be bound by guaranteed messages forwarded by the service provider to the same extent, to the same extent and with the same effect of law as if it had existed in a manually signed form. Likewise, receivers must notify the sender when a message must be routed through the service provider,, must receive guaranteed messages from the service provider, rely on the sender's identity, public key and signature and promptly return a signed receipt to the sender.

<u>Guarantors</u>

Guarantors are required to maintain subscriber records, verify that a sender's private key corresponds to its public key and ensure that subscriber identities and public keys are unique. They must revoke a public key when requested by a subscriber. Guarantors support subscribers by providing first line support and arbitration in the event of a dispute.

Guarantors also confirm guarantees by receiving a guarantee request from the service provider and providing the response in a guarantee response to the service provider.

Guarantors connect to and communicate with the service provider's server and manage the liability risk of its services.

<u>Service Provider</u>

The service provider is required to construct and forward guaranteed messages to the receiver by receiving messages from the server; send guarantee requests to the parties' guarantors; obtain guarantee responses from the guarantors; and construct guaranteed messages from the

signed message if both guarantors confirm the guarantees. Furthermore the service provider is required to receive signed receipts from the receiver and construct and forward a guaranteed receipt to the sender. It is obliged to protect the security of its server and ensure that it can operate at all times and produce evidence to guarantors in the event of disputes.

It will be appreciated that the obligations set out above are merely one example of how the system can work What the subscribers are required to do with their keys is set out in the contract with the guarantor. The role of the service provider may be limited to provide a norm for this contract..

The example described above, and the associated rules, relate specifically to the provision of guaranteed identity by banks. It will be appreciated that the system can be adapted to provide other guarantees without departing from the scope of the invention. Examples include the ability to pay, authorisation and creditworthiness. The message flow and rulebooks for each of these will be different.

Figure 6 illustrates, schematically, the topology of a preferred implementation of the invention. The service supplier is a server which incorporates a message routing function using Internet protocols. The communications between the guarantors and the service provider are preferably across a dedicated communications pathway such as SWIFTNet Interact. The system supports Identrust compliant X.509v3 certificates and applications. The communications between the service provider and the subscribers are via the Internet using standard Internet communications protocols. The messages are preferably sent in XML format with the XML envelope embedding the actual message and X.509v3 certificate.

It will be appreciated from the foregoing that the method and system embodying the invention enable a subscriber to obtain guarantees from its bank, such as confirmation that a certificate issued by the bank and used

to sign an e-commerce message is still valid. The counterparty receiving the message has the guarantee that the identity of the sender has been verified. The receiver has the additional guarantee that the messages have been logged and timestamped by the service provider, which can be relied on in the event of a dispute. The sender has the same benefit as the receiver returns a receipt which is guaranteed by the and logged by the service provider. Businesses may exchange messages over the Internet, or any other communications network via the service provider to enable banks to apply trust, or guarantees, to the receiver when the message is on its way to the receiver.

From the point of view of the financial institution, the method and system embodying the invention provide a platform that banks can use to provide on-line guarantees and e-trust services to corporate customers enabling them to play an active role in B2B e-commerce. The bank can maintain a direct relationship with its customers as they market, sell and support the system using their own e-trust brand, to their customers who sign an agreement with their bank rather than with the service provider. Banks effectively intercept e-commerce messages sent between two businesses and apply guarantees to these messages.

Various modifications and developments beyond those already mentioned are possible and will occur to those skilled in the art without departing from the spirit and scope of the invention.